Available online at www.sciencedirect.com

ScienceDirect

Discrete Mathematics 308 (2008) 3018–3022

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Minimum Lee weights of Type II codes over $\mathbb{F}_{2^r}$

Koichi Betsumiya

Department of Business Information Sciences, Jobu University, Isesaki, Gunma 372-8588, Japan

Received 8 June 2006; accepted 9 August 2007
Available online 3 December 2007

Abstract

Among binary images of a Type II code over $\mathbb{F}_{2^r}$ with respect to the trace-orthogonal bases, it has been unknown whether the minimum Hamming weights depend on the choice of bases or not; the minimum Hamming weights of the binary images of known Type II codes have been independent of the choice of bases.

In this paper we give a complete list of Type II codes over $\mathbb{F}_{64}$ of length 8 up to a certain equivalence. This list shows us an example of a Type II code of which minimum Lee weight depends on the choice of a basis.

Keywords: Self-dual code; Type II code; Lee weight; Trace-orthogonal basis

1. Introduction

There has been much interest in the investigation of binary doubly even self-dual codes, called Type II codes (cf. [14].) The concept of a Type II code has been generalized to self-dual codes over $\mathbb{F}_{2^r}$, and also studied extensively.

As a construction method of binary Type II codes, in 1980s, Pasquier and Wolfmann gave self-dual codes over $\mathbb{F}_{2^r}$ whose binary images with respect to a trace-orthogonal basis (TOB) are binary Type II codes, including the extended Hamming code and the extended Golay code (see [10–12,15–17]). In these papers, extended Reed–Solomon codes and H-codes were widely investigated. More precisely, extended Reed–Solomon codes and H-codes whose binary images are extremal Type II codes of lengths 32, 40 and 64 were constructed (see [12]), and two classes of H-codes whose binary images with respect to a TOB are Type II were found [17].

In 1991, Quebbemann defined "even codes" in [13] as the class of self-dual codes over $\mathbb{F}_{2^r}$ satisfying $\sum_{1\leqslant i<j\leqslant n} v_i v_j = 0$ for any codeword $(v_1, v_2, \ldots, v_n)$. It was shown that the binary image of such a code with respect to any TOB is a Type II code.

In 2000s, the class of self-dual codes over $\mathbb{F}_{2^r}$ whose binary images are Type II codes were studied in [3–5,1]. The class was called Type II codes over $\mathbb{F}_{2^r}$. This definition was shown in [2] to be independent of the choice of a TOB. After that it was shown that the definition of Type II code was equivalent to the even code defined in [13] (cf. [9].) In these papers some basic properties and some classification of Type II codes over $\mathbb{F}_{2^r}$ were given. Type II codes over $\mathbb{F}_4$ of lengths up to 16 were studied in [5,3,1]. The classification of Type II codes over $\mathbb{F}_8$, $\mathbb{F}_{16}$ and $\mathbb{F}_{32}$ of lengths up to 8 was given in [4].

Generally, the Lee weights depend on the choice of a TOB. However, in these papers [3–5,1], we cannot find any Type II code whose minimum Lee weights depend on the choice of a TOB.

E-mail address: betsumi@jobu.ac.jp.

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2007.08.026

The purpose of this paper is the following: the first is to give the classification of Type II codes over $\mathbb{F}_{64}$ of length 8. As a result, we find an example of a Type II code over $\mathbb{F}_{64}$ whose minimum Lee weight depends on the choice of a TOB.

2. Notation and definitions

We denote by $\mathbb{F}_q$ the finite field with q elements. A *code* over $\mathbb{F}_{2^r}$ of length n is a subspace of $\mathbb{F}_{2^r}^n$ as a vector space. An element of a code is called a *codeword*. A code C is self-dual if $u \cdot v = \sum_{i=1}^{n} u_i v_i = 0$ for any codewords $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ of C.

Definition (*Quebbemann [13]*). A *Type II code* over $\mathbb{F}_{2^r}$ of length n is a self-dual code satisfying

$$\sum_{1 \leqslant i < j \leqslant n} v_i v_j = 0$$

for any codeword $v = (v_1, v_2, \ldots, v_n)$.

The symmetric group S_n and the Galois group of $\mathrm{Gal}_{\mathbb{F}_{2^r}/\mathbb{F}_2}$ act on the set of Type II codes over $\mathbb{F}_{2^r}$ of length n. Let C and C' be Type II codes over $\mathbb{F}_{2^r}$ of length n. We say that C' is permutation equivalent to C if $C' = C^\sigma$ for some $\sigma \in S_n$, and C' is equivalent to C if $C' = C^\sigma$ for some $\sigma \in S_n \times \mathrm{Gal}_{\mathbb{F}_{2^r}/\mathbb{F}_2}$. We denote by $\mathrm{PAut}(C) := \{\sigma \in S_n \mid C = C^\sigma\}$ and call it the permutation-automorphism group of C, and by $\mathrm{Aut}(C) := \{\sigma \in S_n \times \mathrm{Gal}_{\mathbb{F}_{2^r}/\mathbb{F}_2} \mid C = C^\sigma\}$ and call it the automorphism group of C.

A basis $B = \{b_1, b_2, \ldots, b_r\}$ of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$ viewed as a vector space over $\mathbb{F}_2$ is called a TOB of $\mathbb{F}_{2^r}$ if $\mathrm{Tr}(b_i b_j) = \delta_{ij}$, where Tr denotes the trace of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$ and δ_{ij} is the Kronecker symbol.

Let $B = \{b_1, b_2, \ldots, b_r\}$ be a TOB of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$. For $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_{2^r}^n$, the binary image $\phi_B(v)$ of v with respect to a basis B is obtained by replacing each component v_i by $(v_i^1, v_i^2, \ldots, v_i^r)$ where $v_i = \sum_{j=1}^{r} v_i^j b_j$. The map ϕ_B is called the Gray map with respect to B. Note that $\phi_B(v)$ depends on the ordering of the elements of B. However, the resulting binary image $\phi_B(C)$ of a code C is determined up to permutation equivalence. The *Lee weight* $\mathrm{wt}_B(v)$ of v with respect to B is defined as the number of components equal to 1 in $\phi_B(v)$. We denote

$$d_B(C) := \mathrm{Min}\{\mathrm{wt}_B(v) \mid v \in C,\ v \neq 0\}$$

and call it the *minimum Lee weight* of C with respect to B.

3. Basic results

In this section, we give properties of Type II codes over $\mathbb{F}_{2^r}$.

Theorem 3.1 (*Betsumiya [2]*). *Let C be a self-dual code over $\mathbb{F}_{2^r}$. Then the following conditions are equivalent*:

1. *C is a Type II code over $\mathbb{F}_{2^r}$.*
2. *For a TOB B, $\phi_B(C)$ is a binary Type II code.*

Theorem 3.2 (*Munemasa [8]*). *The total number of Type II codes over $\mathbb{F}_{2^r}$ of length n is given by*

$$N_{\mathrm{II},r}(n) = \prod_{i=0}^{n/2-2} (2^{ri} + 1) \tag{1}$$

if $rn \equiv 0 \pmod 8$ and $n \equiv 0 \pmod 4$, and 0 otherwise.

Formula (1) is called the mass formula. In Section 4 we will check that the classification is complete by means of the formula from the following corollary.

Corollary 3.3. *Let* $\{C_1, C_2, \ldots, C_t\}$ *be a set of pairwise inequivalent Type II codes over* $\mathbb{F}_{2^r}$ *of length* n. *If the following equality holds*:

$$\sum_{i=1}^{t} \frac{n! \cdot r}{|\mathrm{Aut}(C_i)|} = N_{\mathrm{II},r}(n), \tag{2}$$

then the set gives a complete set of representatives of equivalence classes of Type II codes over $\mathbb{F}_{2^r}$ *of length* n.

4. Classification of Type II codes over $\mathbb{F}_{64}$ of length 8

In this section we will give a complete list of Type II codes over $\mathbb{F}_{64}$ of length 8 up to equivalence.

From now on we denote by α a fixed primitive element of $\mathbb{F}_{64}$ with $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$.

Each C_i $(i = 1, 2, \ldots, 16)$ in Table 1 is a code over $\mathbb{F}_{64}$ of length 8 generated by a matrix $(I\ A)$ where I is the 4×4 identity matrix and A is the 4×4 matrix described in the second to fifth columns. It is easy to see that these codes C_i $(i = 1, 2, \ldots, 16)$ are Type II codes over $\mathbb{F}_{64}$ of length 8. To see that the list gives a complete list of Type II codes over $\mathbb{F}_{64}$ of length 8 up to equivalence, it suffices to verify that, first, these codes are pairwise inequivalent, and, second, Eq. (2) holds.

For $i = 1, 2, 3, 4, 11, 12, 13, 14, 15$ or 16, each C_i is inequivalent to any others, since each of them is characterized by the order of its automorphism group described in the sixth column of Table 1. The automorphism group is calculated as the subset of $S_8 \times \mathrm{Gal}_{\mathbb{F}_{64}/\mathbb{F}_2}$ which stabilizes a given code directly using Magma. For $i = 5, 6, 7, 8, 9, 10$, we have verified their inequivalence by constructing their orbits under the group $S_8 \times \mathrm{Gal}_{\mathbb{F}_{64}/\mathbb{F}_2}$. Hence each one is inequivalent to the others in the list.

Now Eq. (2) is

$$\sum_{i=1}^{16} \frac{8! \cdot 6}{|\mathrm{Aut}(C_i)|} = 532,610 = N_{\mathrm{II},6}(8).$$

Hence Table 1 gives a complete list and the following theorem holds.

Theorem 4.1. *There exist exactly* 16 *Type II codes over* $\mathbb{F}_{64}$ *of length* 8 *up to equivalence*.

The subset $\{0, 1, \alpha^{21}, \alpha^{42}\}$ of $\mathbb{F}_{64}$ forms a subfield, that is, $\mathbb{F}_4$, and the subset $\{0, 1, \alpha^{45}, \alpha^{9}, \alpha^{27}, \alpha^{18}, \alpha^{54}, \alpha^{36}\}$ of $\mathbb{F}_{64}$ form also a subfield, that is, $\mathbb{F}_8$.

Table 1
All Type II codes over $\mathbb{F}_{64}$ of length 8

	First row	Second row	Third row	Fourth row	|Aut|
C_1	$0, \alpha^{39}, \alpha^{31}, \alpha^{33}$	$\alpha^{51}, \alpha^{43}, \alpha^{37}, \alpha^{51}$	$\alpha^{47}, \alpha^{42}, \alpha^{22}, \alpha^{52}$	$\alpha^{48}, \alpha^{8}, \alpha^{6}, \alpha$	$1 \cdot 6$
C_2	$0, \alpha^{13}, \alpha^{41}, \alpha^{36}$	$\alpha^{45}, \alpha^{27}, \alpha^{27}, \alpha^{36}$	$\alpha^{20}, \alpha^{62}, \alpha^{28}, \alpha^{59}$	$\alpha^{34}, \alpha^{35}, \alpha^{55}, \alpha^{31}$	$1 \cdot 2$
C_3	$0, \alpha^{13}, \alpha^{41}, \alpha^{36}$	$\alpha^{39}, \alpha^{11}, \alpha^{23}, \alpha^{39}$	$\alpha^{31}, \alpha^{34}, \alpha^{35}, \alpha^{55}$	$\alpha^{33}, \alpha^{51}, \alpha, \alpha^{52}$	$1 \cdot 1$
C_4	$0, 0, \alpha^{21}, \alpha^{42}$	$\alpha^{13}, \alpha^{10}, \alpha^{53}, \alpha^{32}$	$\alpha^{41}, \alpha^{17}, \alpha^{4}, \alpha^{46}$	$\alpha^{36}, \alpha^{54}, \alpha^{51}, \alpha^{30}$	$3 \cdot 6$
C_5	$\alpha^{13}, \alpha^{45}, \alpha^{12}, \alpha$	$\alpha^{45}, \alpha^{13}, \alpha, \alpha^{12}$	$\alpha^{12}, \alpha, \alpha^{13}, \alpha^{45}$	$\alpha, \alpha^{12}, \alpha^{45}, \alpha^{13}$	$8 \cdot 3$
C_6	$0, \alpha^{39}, \alpha^{31}, \alpha^{33}$	$\alpha^{39}, 0, \alpha^{33}, \alpha^{31}$	$\alpha^{31}, \alpha^{33}, 0, \alpha^{39}$	$\alpha^{33}, \alpha^{31}, \alpha^{39}, 0$	$8 \cdot 3$
C_7	$0, \alpha^{19}, \alpha^{26}, \alpha^{9}$	$\alpha^{19}, 0, \alpha^{9}, \alpha^{26}$	$\alpha^{26}, \alpha^{9}, 0, \alpha^{19}$	$\alpha^{9}, \alpha^{26}, \alpha^{19}, 0$	$8 \cdot 2$
C_8	$\alpha^{33}, \alpha^{37}, \alpha^{25}, \alpha^{55}$	$\alpha^{37}, \alpha^{33}, \alpha^{55}, \alpha^{25}$	$\alpha^{55}, \alpha^{25}, \alpha^{37}, \alpha^{33}$	$\alpha^{25}, \alpha^{55}, \alpha^{33}, \alpha^{37}$	$8 \cdot 2$
C_9	$\alpha^{13}, \alpha^{51}, \alpha^{11}, \alpha^{34}$	$\alpha^{51}, \alpha^{13}, \alpha^{34}, \alpha^{11}$	$\alpha^{11}, \alpha^{34}, \alpha^{13}, \alpha^{51}$	$\alpha^{34}, \alpha^{11}, \alpha^{51}, \alpha^{13}$	$8 \cdot 1$
C_{10}	$\alpha^{13}, \alpha^{27}, \alpha^{62}, \alpha^{35}$	$\alpha^{27}, \alpha^{13}, \alpha^{35}, \alpha^{62}$	$\alpha^{62}, \alpha^{35}, \alpha^{13}, \alpha^{27}$	$\alpha^{35}, \alpha^{62}, \alpha^{27}, \alpha^{13}$	$8 \cdot 1$
C_{11}	$\alpha^{45}, \alpha^{45}, \alpha^{18}, \alpha^{54}$	$\alpha^{45}, \alpha^{27}, \alpha^{36}, \alpha^{27}$	$\alpha^{18}, \alpha^{36}, 1, \alpha^{9}$	$\alpha^{54}, \alpha^{27}, \alpha^{9}, \alpha^{54}$	$56 \cdot 6$
C_{12}	$0, 1, 1, 1$	$1, \alpha^{18}, \alpha^{9}, \alpha^{36}$	$1, \alpha^{9}, \alpha^{36}, \alpha^{18}$	$1, \alpha^{36}, \alpha^{18}, \alpha^{9}$	$96 \cdot 6$
C_{13}	$0, 1, 1, 1$	$1, \alpha^{45}, \alpha^{29}, \alpha^{43}$	$1, \alpha^{29}, \alpha^{43}, \alpha^{45}$	$1, \alpha^{43}, \alpha^{45}, \alpha^{29}$	$96 \cdot 2$
C_{14}	$0, 1, 1, 1$	$1, \alpha^{47}, \alpha^{35}, \alpha^{24}$	$1, \alpha^{35}, \alpha^{24}, \alpha^{47}$	$1, \alpha^{24}, \alpha^{47}, \alpha^{35}$	$96 \cdot 1$
C_{15}	$0, 0, \alpha^{21}, \alpha^{42}$	$0, 0, \alpha^{42}, \alpha^{21}$	$\alpha^{21}, \alpha^{42}, 0, 0$	$\alpha^{42}, \alpha^{21}, 0, 0$	$288 \cdot 6$
C_{16}	$0, 1, 1, 1$	$1, 0, 1, 1$	$1, 1, 0, 1$	$1, 1, 1, 0$	$1344 \cdot 6$

The codes C_{11}, C_{12}, C_{15} and C_{16} can be defined as Type II codes over the subfields $\mathbb{F}_8$, $\mathbb{F}_8$, $\mathbb{F}_4$ and $\mathbb{F}_2$, respectively. C_{16} is the extended Hamming code over $\mathbb{F}_2$. C_{15} is the direct sum of a pair of the unique Type II codes over $\mathbb{F}_8$ of length 4. C_{12} and C_{11} are the Type II codes $C_{8,2}$ and $C_{8,3}$ in [4], respectively.

5. Minimum Lee weights

In this section we discuss the minimum Lee weights of the codes in the previous section. The Lee weight is defined with respect to a TOB, hence it depends on the choice of a TOB. However, it has not been known whether there actually exists an example of a Type II code over $\mathbb{F}_{2^r}$ whose minimum Lee weights depend on the choice of a TOB or not (cf. [4].) Here, we show that such an example is found among the Type II codes over $\mathbb{F}_{64}$ classified in the previous section.

The total number of TOBs of $\mathbb{F}_{2^r}/\mathbb{F}_2$ is $2^{r-1}|\mathrm{Sp}(r-2,2)|/r!$ if r is even, $|\mathrm{Sp}(r-1,2)|/r!$ otherwise, where $\mathrm{Sp}(r,2)$ is the symplectic group of degree r over $\mathbb{F}_2$ (cf. [7]). The order of $\mathrm{Sp}(2m,2)$ is known (cf. [6]) to be

$$|\mathrm{Sp}(2m,2)| = 2^{m^2}\prod_{i=1}^{m}(2^{2i}-1).$$

Hence, there are 32 TOBs of $\mathbb{F}_{64}/\mathbb{F}_2$, and they are given as $\{B_1, B_2\} \cap \{B_i^{2^j} \mid i = 3, 4;\ j = 1, 2, 3\} \cap \{B_i^{2^j} \mid i = 5, 6, 7, 8;\ j = 1, 2, 3, 4, 5, 6\}$ where

$$\begin{aligned}
B_1 &= \{\alpha^{13}, \alpha^{38}, \alpha^{19}, \alpha^{41}, \alpha^{52}, \alpha^{26}\},\\
B_2 &= \{\alpha^{3}, \alpha^{33}, \alpha^{48}, \alpha^{24}, \alpha^{12}, \alpha^{6}\},\\
B_3 &= \{\alpha^{25}, \alpha^{38}, \alpha^{43}, \alpha^{11}, \alpha^{52}, \alpha^{29}\},\\
B_4 &= \{\alpha^{25}, \alpha^{24}, \alpha^{53}, \alpha^{11}, \alpha^{3}, \alpha^{46}\},\\
B_5 &= \{\alpha^{25}, \alpha^{26}, \alpha^{47}, \alpha^{31}, \alpha^{52}, \alpha^{46}\},\\
B_6 &= \{\alpha^{25}, \alpha^{42}, \alpha^{48}, \alpha^{31}, \alpha^{3}, \alpha^{29}\},\\
B_7 &= \{\alpha^{25}, \alpha^{43}, \alpha^{48}, \alpha^{47}, \alpha^{24}, \alpha^{55}\},\\
B_8 &= \{\alpha^{25}, \alpha^{38}, \alpha^{42}, \alpha^{26}, \alpha^{53}, \alpha^{55}\}.
\end{aligned}$$

The minimum Lee weights of C_i for $i = 1, 2, 3, 5, 6, 7, 8, 9, 10$ and 11 are 8 with respect to all TOBs. The minimum Lee weights of C_i for $i = 12, 13, 14, 15$ and 16 are 4 with respect to all TOBs. The minimum Lee weight of C_4 is 8 with respect to B_1, B_3, B_6, B_7, B_8, and is 4 with respect to B_2, B_4, B_5. That is, C_4 is an example of a Type II code of length 8 over $\mathbb{F}_{64}$ whose minimum Lee weight depends on the choice of a TOB.

Acknowledgement

The author thanks A. Munemasa and M. Harada for many useful comments to calculate these results. This work was done during a visit in 2001 by the author to the Institute for Mathematical Sciences of the National University of Singapore on a grant from the DSTA of Singapore. The author is grateful to the Institute for its support and kind hospitality. This work was partially supported by the MEXT, Japan, Grant-in-Aid for Young Scientists (B) (16740023).

References

[1] K. Betsumiya, On the classification of Type II codes over $\mathbb{F}_{2^r}$ with binary length 32, preprint, 2001.
[2] K. Betsumiya, The Type II property for self-dual codes over finite fields of characteristic two, preprint, 2001.
[3] K. Betsumiya, T.A. Gulliver, M. Harada, A. Munemasa, On type II codes over $\mathbb{F}_4$, IEEE Trans. Inform. Theory 47 (6) (2001) 2242–2248.
[4] K. Betsumiya, M. Harada, A. Munemasa, Type II codes over $\mathbb{F}_{2^r}$, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Melbourne, 2001, Lecture Notes in Computer Science, vol. 2227, Springer, Berlin, 2001, pp. 102–111.
[5] P. Gaborit, V. Pless, P. Solé, O. Atkin, Type II codes over $\mathbb{F}_4$, Finite Fields Appl. 8 (2) (2002) 171–183.
[6] L.C. Grove, Classical Groups and Geometric Algebra, Graduate Studies in Mathematics, vol. 39, American Mathematical Society, Providence, RI, 2002.
[7] D. Jungnickel, Finite Fields, Structure and Arithmetics, Bibliographisches Institut, Mannheim, 1993.

[8] A. Munemasa, A mass formula for Type II codes over finite fields of characteristic two, in: Codes and Designs, Columbus, OH, 2000, vol. 10, Ohio State University Mathematical Research Institute Publications, de Gruyter, Berlin, 2002, pp. 207–214.
[9] G. Nebe, H.-G. Quebbemann, E.M. Rains, N.J.A. Sloane, Complete weight enumerators of generalized doubly-even self-dual codes, Finite Fields Appl. 10 (4) (2004) 540–550.
[10] G. Pasquier, The binary GOLAY code obtained from an extended cyclic code over $\mathbf{F}_8$, European J. Combin. 1 (4) (1980) 369–370.
[11] G. Pasquier, Binary images of some self-dual codes over GF(2^m) with respect to trace-orthogonal basis, Discrete Math. 37 (1) (1981) 127–129.
[12] G. Pasquier, Binary self-dual codes construction from self-dual codes over a Galois field $\mathbf{F}_{2^m}$, in: Combinatorial Mathematics, Marseille-Luminy, 1981, North-Holland Mathematics Studies, vol. 75, North-Holland, Amsterdam, 1983, pp. 519–526.
[13] H.-G. Quebbemann, On even codes, Discrete Math. 98 (1) (1991) 29–34.
[14] E.M. Rains, N.J.A. Sloane, Self-dual codes, in: Handbook of Coding Theory, vols. I and II, North-Holland, Amsterdam, 1998, pp. 177–294.
[15] J. Wolfmann, A new construction of the binary Golay code (24, 12, 8) using a group algebra over a finite field, Discrete Math. 31 (3) (1980) 337–338.
[16] J. Wolfmann, A class of doubly even self-dual binary codes, Discrete Math. 56 (2–3) (1985) 299–303.
[17] J. Wolfmann, A group algebra construction of binary even self-dual codes, Discrete Math. 65 (1) (1987) 81–89.